PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-200196
(43)Date of publication of application : 31.07.1997

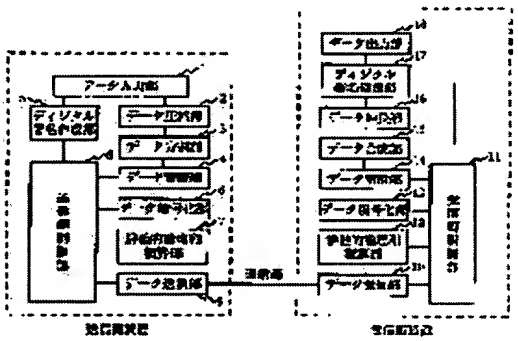
(51)Int.CI. H04L 9/18
G09C 1/00
H04L 9/34

(21)Application number : 08-010105
(22)Date of filing : 24.01.1996

(71)Applicant : BROTHER IND LTD
(72)Inventor : NAKAMURA MICHIHIRO

(54) CIPHERING COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To attain high speed processing by applying ciphering processing to only 1st division data and applying exclusive OR arithmetic operation to 2nd to final n-th division data.
SOLUTION: Data given to a transmitter are given to a data compression section 2, in Which compression processing is conducted and compressed data are divided for 128-bit each by a data division section 3, in which n-sets of division data are generated and stored in a data storage section 4. Then only 1st division data among the division data are subject to ciphering processing at a data ciphering section 6 by using a public key of a recipient (b) and the remaining division data are calculated by an exclusive OR arithmetic section 7 and then the division data are generated and the data are sent by a data transmission section 9 with a digital signature. A data decoding section 13 of a receiver side decodes the 1st division transmission data by using a secret key of a recipient (b) and the 1st division data are decoded and the remaining division transmission data are calculated by an exclusive OR arithmetic section 12 and the division data are decoded.



LEGAL STATUS

[Date of request for examination] 18.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Citation 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平9－200196

(43)公開日　平成９年(1997)７月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04L 9/18			H04L 9/00	651	
G09C 1/00	610	7259-5J	G09C 1/00	610	D
H04L 9/34			H04L 9/00	681	

審査請求　未請求　請求項の数６　ＯＬ　（全８頁）

(21)出願番号　特願平8－10105

(22)出願日　平成８年(1996)１月24日

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番１号

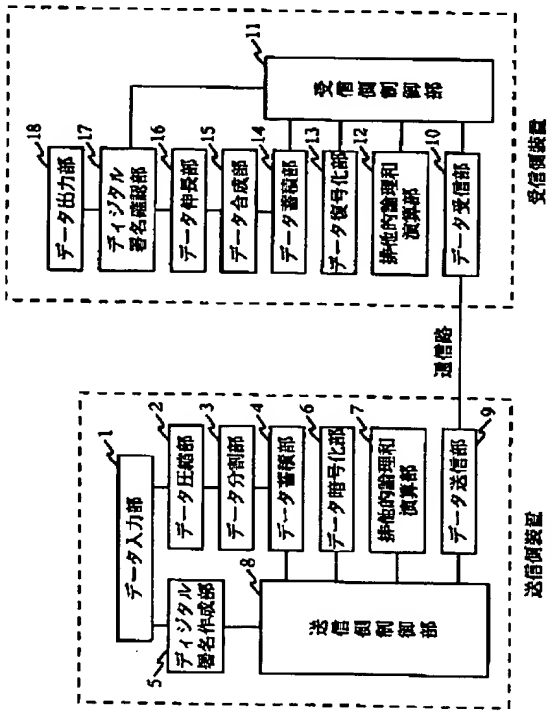
(72)発明者　中村　道弘
名古屋市瑞穂区苗代町15番１号ブラザー工業株式会社内

(54)【発明の名称】暗号通信方式

(57)【要約】

【課題】　通信データ本文全体を暗号化処理する場合よりも短い時間で通信処理を完了することができる暗号通信方式を提供することである。

【解決手段】　送信側では、通信データ本文全体を特定のビット毎にｎ個に分割し、その第１分割データを暗号化処理して送信データとすると共に、第１分割データと第２分割データとの組から最後の第ｎ－１分割データと第ｎ分割データとの組まで順次排他的論理和を計算して第２分割データから第ｎ分割データまでの送信データを求め、それ等全ての送信データを受信側に送信する一方、受信側では、受信した第１分割送信データを復号処理して元の第１分割データを求めると共に、受信した第２分割送信データから第ｎ分割データについては前記各組毎に排他的論理和を計算して元の第２分割データから第ｎ分割データまでを求め、これ等求められた全ての分割データを合成して元の通信データに復元する。



1

【特許請求の範囲】

【請求項１】　通信データを送信側で暗号化して受信側に送信するようにした暗号通信方式において、

前記送信側では、

通信データの全体を特定のビット長さ毎にｎ（２≦ｎ）個に分割して、その分割された第１分割データと第２分割データとの組の排他的論理和を計算して第２分割データの送信データを求め、以降、同様にして第ｎ－１分割データと第ｎ分割データとの組まで順次排他的論理和を計算して第ｎ分割データまでの各送信データを求める一方、前記第１分割データを暗号化処理して送信可能な暗号化データとし、その暗号化された第１分割送信データ及び前記排他的論理和演算された第２分割送信データから第ｎ分割送信データまでの各送信データを前記受信側に送信し、

前記受信側では、

前記送信側から送信された各通信データを受信して、前記暗号化された第１分割送信データを復号処理して元の第１分割データを求めると共に、前記第２分割送信データと前記復号した第１分割データとの組の排他的論理和を計算して元の第２分割データを求め、以降、同様にして第ｎ分割送信データと復元した第ｎ－１分割データとの組まで順次排他的論理和を計算して元の第ｎ分割データまで求めた後、前記第１分割データから第ｎ分割データまでを合成して元の通信データを復元することを特徴とする暗号通信方式。

【請求項２】　通信データを送信側で暗号化して受信側に送信するようにした暗号通信方式において、

前記送信側では、

通信データの全体を特定のビット長さ毎にｎ（３≦ｎ）個に分割して、その分割された途中の第ｉ分割データ（２≦ｉ≦ｎ－１）と第ｉ＋１分割データとの組の排他的論理和を計算して第ｉ＋１分割データの送信データを求め、以降、同様にして第ｎ－１分割データと第ｎ分割データとの組まで順次排他的論理和を計算して第ｎ分割データまでの各送信データを求める一方、第１分割データから前記第ｉ分割データまでの各分割データを暗号化処理して送信可能な各暗号化データとし、その暗号化された第１分割送信データから第ｉ分割送信データまでの各送信データ及び前記排他的論理和演算された第ｉ＋１分割送信データから第ｎ分割送信データまでの各送信データを前記受信側に送信し、

前記受信側では、

前記送信側から送信された各通信データを受信して、前記暗号化された第１分割送信データから第ｉ分割送信データまでの各送信データを復号処理して元の第１分割データから第ｉ分割データまでの各分割データを求めると共に、前記第ｉ＋１分割送信データと前記復号した第ｉ分割データとの組の排他的論理和を計算して元の第ｉ＋１分割データを求め、以降、同様にして第ｎ分割送信データと復元した第ｎ－１分割データとの組まで順次排他的論理和を計算して元の第ｎ分割データまで求めた後、前記第１分割データから第ｎ分割データまでを合成して元の通信データを復元することを特徴とする暗号通信方式。

2

【請求項３】　前記送信側では、通信データを分割する前にその通信データの圧縮処理を行なうと共に、その圧縮通信データを分割して分割データとし、前記受信側では、前記分割データを合成して元の圧縮通信データを求め、その圧縮通信データを伸長処理して元の通信データに復元することを特徴とする請求項１または２に記載の暗号通信方式。

【請求項４】　前記暗号化処理は公開鍵暗号方式を用いたことを特徴とする請求項１乃至３のいずれかに記載の暗号通信方式。

【請求項５】　前記暗号化処理は慣用鍵暗号方式を用いたことを特徴とする請求項１乃至３のいずれかに記載の暗号通信方式。

【請求項６】　前記送信側では、通信データの全体を特定の長さに圧縮するハッシュ処理を行なうと共に、送信者のディジタル署名を作成して前記受信側に送信し、前記受信側では、復元された通信データの全体についてハッシュ処理を行なうと共に、受信した送信者のディジタル署名を復号し、前記各ハッシュ処理の結果が一致すれば、通信データ及び送信者が正当であるとして処理することを特徴とする請求項１及至５のいずれかに記載の暗号通信方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化されたデータを送受信する暗号通信方式に係り、特に、送信するデータの一部分のみを暗号化することによってデータ全体を暗号化した場合と同様の機密性を保つことができる暗号通信方式に関するものである。

【０００２】

【従来の技術】近年、通信ネットワークの凄まじい発展によりさまざまなデータがネットワークを介して通信されるようになってきている。これらのネットワークには、ネットワーク上での盗聴、通信データの改ざん、送信者を偽るなりすまし等のセキュリティ上の問題が存在している。このようなネットワーク通信路上のデータのセキュリティ確保のために、暗号化したデータを通信する暗号通信方式が幅広く用いられるようになってきている。

【０００３】

【発明が解決しようとする課題】しかしながら、従来の暗号通信方式では、通信データの本文全体が暗号化処理されていたために、通常の暗号化処理を行なわない通信に比較して通信処理に時間がかかるという問題点があった。

【０００４】本発明は、上述した問題点を解決するためになされたものであり、通信データの一部分のみに暗号化処理を行なうことによって、通信データの本文全体を暗号化処理した場合と同等の機密性を維持しつつ、短い時間で通信処理を完了することができる暗号通信方式を提供することを目的とする。

【０００５】

【課題を解決するための手段】この目的を達成するために、本発明の請求項１に記載の暗号通信方式は、通信データを送信側で暗号化して受信側に送信するようにした方式を対象として、特に、前記送信側では、通信データの全体を特定のビット長さ毎にｎ（２≦ｎ）個に分割して、その分割された第１分割データと第２分割データとの組の排他的論理和を計算して第２分割データの送信データを求め、以降、同様にして第ｎ－１分割データと第ｎ分割データとの組まで順次排他的論理和を計算して第ｎ分割データまでの各送信データを求める一方、前記第１分割データを暗号化処理して送信可能な暗号化データとし、その暗号化された第１分割送信データ及び前記排他的論理和演算された第２分割送信データから第ｎ分割送信データまでの各送信データを前記受信側に送信する。

【０００６】そして、前記受信側では、前記送信側から送信された各通信データを受信して、前記暗号化された第１分割送信データを復号処理して元の第１分割データを求めると共に、前記第２分割送信データと前記復号した第１分割データとの組の排他的論理和を計算して元の第２分割データを求め、以降、同様にして第ｎ分割送信データと復元した第ｎ－１分割データとの組まで順次排他的論理和を計算して元の第ｎ分割データまで求めた後、前記第１分割データから第ｎ分割データまでを合成して元の通信データを復元する。

【０００７】従って、通信データを分割して第１分割データのみを暗号化処理し、第２分割データから第ｎ分割データまでを排他的論理和演算を行なうことによって通信データの機密性を保つことができるものである。また、暗号化処理はひとつの分割データのみであり、他の分割データは簡単な排他的論理和のビット演算であるので、高速な処理が可能になる。

【０００８】また、請求項２に記載の暗号通信方式は、通信データを送信側で暗号化して受信側に送信するようにした方式を対象として、特に、前記送信側では、通信データの全体を特定のビット長さ毎にｎ（３≦ｎ）個に分割して、その分割された途中の第ｉ分割データ（２≦ｉ≦ｎ－１）と第ｉ＋１分割データとの組の排他的論理和を計算して第ｉ＋１分割データの送信データを求め、以降、同様にして第ｎ－１分割データと第ｎ分割データとの組まで順次排他的論理和を計算して第ｎ分割データまでの各送信データを求める一方、第１分割データから前記第ｉ分割データまでの各分割データを暗号化処理して送信可能な各暗号化データとし、その暗号化された第１分割送信データから第ｉ分割送信データまでの各送信データ及び前記排他的論理和演算された第ｉ＋１分割送信データから第ｎ分割送信データまでの各送信データを前記受信側に送信する。

【０００９】そして、前記受信側では、前記送信側から送信された各通信データを受信して、前記暗号化された第１分割送信データから第ｉ分割送信データまでの各送信データを復号処理して元の第１分割データから第ｉ分割データまでの各分割データを求めると共に、前記第ｉ＋１分割送信データと前記復号した第ｉ分割データとの組の排他的論理和を計算して元の第ｉ＋１分割データを求め、以降、同様にして第ｎ分割送信データと復元した第ｎ－１分割データとの組まで順次排他的論理和を計算して元の第ｎ分割データまで求めた後、前記第１分割データから第ｎ分割データまでを合成して元の通信データを復元する。

【００１０】従って、分割した通信データの第１分割データから第ｉ分割データを暗号化処理し、第ｉ＋１分割データから第ｎ分割データまでを排他的論理和演算を行なうことによって、通信データの最初の部分が特定のフォーマットにされている場合に一つの分割データの暗号化処理のみでは常に同じ暗号化データになる危険性を避けることができ、通信データの機密性の向上を強化することができるものである。

【００１１】また、請求項３に記載の暗号通信方式は、前記送信側では、通信データを分割する前にその通信データの圧縮処理を行ない、その圧縮通信データを分割して分割データとし、前記受信側では、前記分割データを合成して元の圧縮通信データを求め、その圧縮通信データを伸長処理して元の通信データに復元する。従って、通信データ本文全体を圧縮処理することによって、通信データの容量を減らすことができ、通信時間及び通信処理時間を短縮することができるものであり、また、圧縮処理されたデータ自体は、通信データ本文の内容を伸長処理しない限り意味をなさないランダムデータとなっているので、排他的論理和演算処理部分のデータの機密性を暗号化処理を行なったものと同等にすることができるものである。

【００１２】また、請求項４に記載の暗号通信方式は、前記暗号化処理として、公開鍵暗号方式を用いている。従って、通信者間で暗号通信を行なう際に事前に暗号鍵を共有しておく必要がなく、通信相手の公開鍵をお互いに持つことで暗号通信を行なうことができるものである。

【００１３】また、請求項５に記載の暗号通信方式は、前記暗号化処理として、慣用鍵暗号方式を用いている。従って、公開鍵暗号方式よりも高速に暗号化処理を行なうことができるものである。また、大量の暗号文と平文の組を利用する差分攻撃法や線形攻撃法に対して、１回

の通信に使用される暗号文と平文の組は、１組か数組のごく少ないものであるので、差分攻撃法や線形攻撃法に必要な数の暗号文と平文の組を入手するには非常に時間がかかるために安全性に優れている。

【００１４】さらに、請求項６に記載の暗号通信方式は、前記送信側では、通信データの全体を特定の長さに圧縮するハッシュ処理を行なうと共に、送信者のディジタル署名を作成して前記受信側に送信し、前記受信側では、復元された通信データの全体についてハッシュ処理を行なうと共に、受信した送信者のディジタル署名を復号し、前記各ハッシュ処理の結果が一致すれば、通信データ及び送信者が正当であるとして処理する。従って、通信データの本文のディジタル署名を送信することによって、通信データと送信者とが正当であることを確認することができるものである。

【００１５】

【発明の実施の形態】以下に、本発明の暗号通信方式を具体化した実施の形態について図面を参照して説明する。

【００１６】図１は、本発明の暗号通信方式を適用した通信装置の構成を示すブロック図である。

【００１７】送信側装置は、データ入力部１、データ圧縮部２、データ分割部３、データ蓄積部４、ディジタル署名作成部５、データ暗号化部６、排他的論理和演算部７、送信側制御部８及びデータ送信部９から構成される。また、受信側装置は、データ受信部１０、受信側制御部１１、排他的論理和演算部１２、データ復号化部１３、データ蓄積部１４、データ合成部１５、データ伸長部１６、ディジタル署名確認部１７及びデータ出力部１８から構成される。

【００１８】前記データ入力部１は、コンピュータ上等で作成・編集された文章やデータ等を送信側装置に入力するためのインターフェイスである。

【００１９】前記データ圧縮部２は、入力データを特定の圧縮フォーマットに従って圧縮処理を行なうものである。

【００２０】前記データ分割部３は、圧縮されたデータを１２８ビット毎に分割するものであり、ｎ個の分割データ（Ｄ１，．．．．．，Ｄｎ）を作成するものであるが、最後の第ｎ分割データ（Ｄｎ）は１２８ビットちょうどでなくても構わない。

【００２１】前記データ蓄積部４は、暗号化処理及び排他的論理和演算を行なうために分割データを一時的に蓄積しておくものである。

【００２２】前記ディジタル署名作成部５は、暗号／復号処理方式に公開鍵暗号方式を使用するものであり、入力されたデータ本文全体にハッシュ処理、即ち、通信データの全体を特定の長さに圧縮する処理を行ない、ハッシュデータ（ＨＤ）を作成し、このハッシュデータを次の式

ＨＤ’　＝　ＥＫＥｂ［ＤＫＤａ（ＨＤ）］

のように、送信者ａの秘密鍵（ＫＤａ）を用いて復号化処理したものを受信者ｂの公開鍵（ＫＥｂ）を用いてさらに暗号化処理を行なって、送信者ａの認証と送信データの正当性を証明するためのディジタル署名（ＨＤ’）を作成するものである。ここで、前記ＥＫＥｂは受信者ｂの公開鍵（ＫＥｂ）を用いる暗号化処理、前記ＤＫＤａは送信者ａの秘密鍵（ＫＤａ）を用いる復号化処理である。

【００２３】前記データ暗号化部６は、データの暗号／復号処理方式に公開鍵暗号方式を使用するものであり、受信者ｂの公開鍵（ＫＥｂ）を用いて

Ｄ１’　＝　ＥＫＥｂ（Ｄ１）

のように、第１分割データ（Ｄ１）の暗号化処理を行ない、第１分割送信データ（Ｄ１’）を作成するものである。

【００２４】前記排他的論理和演算部７は、第２分割データ（Ｄ２）から第ｎ分割データ（Ｄｎ）までを、次の式

Ｄｉ’　＝　Ｄｉ　＾　Ｄｉ－１　（２≦ｉ≦ｎ）

を用いて、排他的論理和演算を行ない、分割送信データ（Ｄ２’，．．．，Ｄｎ’）を作成するものである。ここで、＾はビット毎の排他的論理和演算であり、以降の式の＾も同様の排他的論理和演算である。

【００２５】前記送信側制御部８は、送信側装置全体の制御処理を実行するものであって、暗号通信を行なうための制御、通信手順における諸々の制御を実行するものである。

【００２６】前記データ送信部９は、ディジタル署名データと共に作成された分割送信データの第１分割送信データ（Ｄ１’）から第ｎ分割送信データ（Ｄｎ’）までを順次送信するものである。

【００２７】前記データ受信部１０は、通信路を介して送信されたデータを受信するものである。

【００２８】前記受信側制御部１１は、受信側装置全体の制御処理を実行するものであり、暗号通信を行なうための制御、通信手順における諸々の制御を実行するものである。

【００２９】データ復号化部１３は、データ暗号化部６と同様にデータの暗号／復号処理方式に公開鍵暗号方式を使用するものであり、受信者ｂの秘密鍵（ＫＤｂ）を用いて

Ｄ１　＝　ＤＫＤｂ（Ｄ１’）

のように、第１分割送信データ（Ｄ１’）の復号化処理を行ない、第１分割データ（Ｄ１）を復号するものである。ここで、前記ＤＫＤｂは受信者ｂの秘密鍵（ＫＤｂ）を用いる復号化処理である。

【００３０】前記排他的論理和演算部１２は、データ復号化部１３で復号された第１分割データ（Ｄ１）を初期値として、第２分割送信データ（Ｄ２’）から第ｎ分割

送信データ（Ｄｎ’）までを、次の式
Ｄｉ　＝　Ｄｉ’　＾　Ｄｉ－１　（２≦ｉ≦ｎ）
を用いて、排他的論理和演算を行ない、分割データ（Ｄ２，．．．，Ｄｎ）を復元するものである。

【００３１】前記データ蓄積部１４は、分割データの合成を行なうために、復元された分割データを一時的に蓄積しておくものである。

【００３２】前記データ合成部１５は、復元された分割データを元のひとつの圧縮通信データに合成するための処理を行なうものである。

【００３３】前記データ伸長部１６は、合成された圧縮通信データに伸長処理を施して元の通信データに復元するものである。

【００３４】ディジタル署名確認部１７は、暗号／復号処理方式に公開鍵暗号方式を使用するものであり、データ伸長部１６で復元された通信データ本文全体のハッシュ処理を行ない、ハッシュデータ（ＨＤ１）を求め、受信したディジタル署名（ＨＤ’）を次の式
ＨＤ　＝　ＥＫＥａ［ＤＫＤｂ（ＨＤ’）］
のように、受信者ｂの秘密鍵（ＫＤｂ）を用いて復号化処理したものを送信者ａの公開鍵（ＫＥａ）を用いてさらに暗号化処理を行なって、送信者ａが作成したハッシュデータ（ＨＤ）を取り出し、二つのハッシュデータ（ＨＤ１とＨＤ）の値を照合して一致するか否かを確認し、一致する場合には送信者ａの認証と送信データとが正当であることを証明し、一致しない場合には途中でデータが改ざんされたか、送信者ａを偽ったなりすましが行なわれたとの判断を行なうものである。ここで、前記ＥＫＥａは送信者ａの公開鍵（ＫＥａ）を用いる暗号化処理である。

【００３５】前記データ出力部１８は、ディジタル署名確認部１７で送信者ａの認証と送信データとが正当であることが証明された場合には復元した通信データを出力し、送信者ａの認証と送信データとが正当であることが証明されなかった場合にはエラーメッセージを出力するものである。

【００３６】このような構成を有する本実施の形態の通信装置に基づく暗号通信方式の送信手順を図２のフローチャートを用いて説明する。

【００３７】なお、送信者ａと受信者ｂの間で通信を開始する前に、送信者ａと受信者ｂとは、お互いの公開鍵（ＫＥａ、ＫＥｂ）を入手しておく必要があるが、公開鍵の入手方法は、どのような方法を用いても構わない。

【００３８】先ず、送信者ａは、受信者ｂに送りたいデータをコンピュータ上等で作成し、データ入力部１のインターフェイスを介して送信装置に入力する（Ｓ１）。入力されたデータは、ディジタル署名作成部５によってデータ本文全体についてハッシュ処理が施され、ハッシュデータ（ＨＤ）が作成される。このハッシュデータは、送信者ａの秘密鍵（ＫＤａ）と受信者ｂの公開鍵（ＫＥｂ）とを用いて
ＨＤ’　＝　ＥＫＥｂ［ＤＫＤａ（ＨＤ）］
のように暗号化処理がなされて、ディジタル署名（ＨＤ’）が作成されるのである（Ｓ２）。このディジタル署名は、受信側で送信者ａの認証と送信データの正当性を証明するために使用される。

【００３９】入力されたデータは、データ圧縮部２によって圧縮処理が施され（Ｓ３）、圧縮データが作成される。この圧縮データは、入力データサイズよりも小さなサイズとなり、通信データを縮小することができる。圧縮データは、データ分割部３によって１２８ビット毎に分割され（Ｓ４）、ｎ個の分割データ（Ｄ１，．．．，Ｄｎ）が作成され、データ蓄積部４に蓄積される。分割データの内の第１分割データ（Ｄ１）のみがデータ暗号化部６によって、受信者ｂの公開鍵（ＫＥｂ）を用いて
Ｄ１’　＝　ＥＫＥｂ（Ｄ１）
のように、暗号化処理されて（Ｓ５）、第１分割送信データ（Ｄ１’）が作成される。残りの分割データは、排他的論理和演算部７によって、
Ｄｉ’　＝　Ｄｉ　＾　Ｄｉ－１　（２≦ｉ≦ｎ）
の演算を施されて（Ｓ６）、分割送信データ（Ｄ２’，．．．，Ｄｎ’）が作成される。

【００４０】作成された分割送信データ（Ｄ１’，．．．，Ｄｎ’）は、ディジタル署名（ＨＤ’）と共にデータ送信部９によって送信される（Ｓ７）。

【００４１】次に、本実施の形態の通信装置における暗号通信方式の受信手順を図３のフローチャートを用いて説明する。

【００４２】通信路を介して送信者ａから送信されたデータは、データ受信部１０によって受信され（Ｓ１１）、第１分割送信データ（Ｄ１’）は、データ復号化部１３によって、受信者ｂの秘密鍵（ＫＤｂ）を用いて
Ｄ１　＝　ＤＫＤｂ（Ｄ１’）
のように、復号化処理が施され（Ｓ１２）、第１分割データ（Ｄ１）が復号される。残りの分割送信データ（Ｄ２’，．．．，Ｄｎ’）は、排他的論理和演算部１２によって、
Ｄｉ　＝　Ｄｉ’　＾　Ｄｉ－１　（２≦ｉ≦ｎ）
の演算が施されて（Ｓ１３）、分割データ（Ｄ２，．．．，Ｄｎ）がそれぞれ復元される。

【００４３】復元された分割データ（Ｄ１，．．．，Ｄｎ）は、データ合成部１５によって合成されて（Ｓ１４）、元の圧縮データに復元される。この復元された圧縮データは、データ伸長部１６によって伸長処理が施され（Ｓ１５）、元の通信データに復元される。復元された通信データは、送信側と同じハッシュ処理が施され（Ｓ１６）、ハッシュデータ（ＨＤ１）が作成される。

【００４４】また、受信されたディジタル署名（ＨＤ’）は、受信者ｂの秘密鍵（ＫＤｂ）と送信者ａの公開鍵（ＫＥａ）を用いて

ＨＤ　＝　ＥＫＥａ［ＤＫＤｂ（ＨＤ’）］
のように復号化処理されて（Ｓ１７）、送信者ａが作成したハッシュデータ（ＨＤ）が取り出される。この二つのハッシュデータ（ＨＤ１とＨＤ）は、ディジタル署名確認部１７によって、値が一致するか否かが調べられ（Ｓ１８）、一致する場合（Ｓ１８：ＹＥＳ）には送信者ａの認証と送信データとが正当であることが証明され、データ出力部１８によって、復元した通信データが出力される（Ｓ１９）。一方、一致しない場合（Ｓ１８：ＮＯ）には、途中でデータが改ざんされたか、送信者ａを偽ったなりすましが行なわれたと判断され、データ出力部１８によって、エラーメッセージが出力される（Ｓ２０）。

【００４５】本発明は、前記実施の形態に限定されることなく、その趣旨を逸脱しない範囲内で種々の変更が可能である。

【００４６】即ち、前記実施の形態では、送信側において通信データの分割処理の前に圧縮処理を行ない、受信側において圧縮通信データを伸長処理して復元するようにしているが、圧縮せずに平文のまま通信データの分割処理を行なって送信することも可能である。

【００４７】また、前記実施の形態では、ｎ個に分割された分割データの内の最初の一つの分割データのみを暗号化処理して送信データとすると共に、残りの全ての分割データを排他的論理和演算して送信データとしたが、分割数ｎより小さい数（例えば、分割数２０個の内、最初から連続する３個とか５個）の複数の分割データを暗号化処理してそれぞれ送信データとし、その暗号化処理する最後の分割データの次の分割データから最後の第ｎ分割データまでの各分割データについては、前記実施の形態と同様に排他的論理和を計算してそれぞれ送信データを求め、これ等暗号化処理した各送信データと排他的論理和演算された各送信データとを受信側に送信する一方、受信側では、前記実施の形態と同様に、前記暗号化処理した各送信データを複合処理してそれぞれ元の各分割データを求めると共に、前記排他的論理和演算された各送信データについては排他的論理和演算してそれぞれ元の各分割データを求め、これ等求められた最初の分割データから第ｎ分割データまでの全ての分割データを合成して元の通信データに復元するように構成してもよい。

【００４８】また、前記実施の形態では、暗号化処理の方式に公開鍵暗号方式を使用したが、慣用鍵暗号方式を使用することも可能である。

【００４９】さらに、前記実施の形態では、送信側通信装置と受信側通信装置とを別々に構成しているが、送信側通信装置と受信側通信装置の各々の機能を一つの通信装置で構成することも可能である。

【００５０】

【発明の効果】以上説明したことから明かなように、本発明の請求項１に記載の暗号通信方式によれば、通信データを分割して第１分割データのみを暗号化処理し、第２分割データから最後の第ｎ分割データを排他的論理和演算を行なうことによって通信データの機密性を保つことができるものである。また、暗号化処理は一つの分割データのみであり、他の分割データは簡単な排他的論理和のビット演算であるので、高速な処理が可能になり、暗号化処理に専用のハードウエアを用意することなく、ソフトウエアのみで装置を構成することができ、通信装置のコストを低減させることができるものである。

【００５１】また、請求項２に記載の暗号通信方式によれば、分割した通信データの第１分割データから第ｉ分割データまでを暗号化処理し、第ｉ＋１分割データから第ｎ分割データを排他的論理和演算を行なうことによって、特に、通信データの最初の部分が特定のフォーマットにされているような場合に、一つの分割データの暗号化処理のみでは常に同じ暗号化データになる危険性を避けることができるものであり、通信データの機密性の向上を強化することができるものである。

【００５２】また、請求項３に記載の暗号通信方式によれば、通信データの本文全体を圧縮処理することによって、通信データの容量を減らすことができ、通信時間及び通信処理時間を短縮することができるものであり、また、圧縮処理されたデータ自体は、通信データ本文の内容を伸長処理しない限り意味をなさないランダムデータとなっているので、排他的論理和演算処理部分のデータの機密性を暗号化処理を行なったものと同等にすることができるものである。

【００５３】また、請求項４に記載の暗号通信方式によれば、暗号化処理方式に公開鍵暗号方式を使用することによって、通信者間で暗号通信を行なう際に事前に暗号鍵を共有しておく必要がなく、通信相手の公開鍵をお互いに持つことで暗号通信を行なうことができるものである。

【００５４】また、請求項５に記載の暗号通信方式によれば、暗号化処理方式に慣用鍵暗号方式を使用することにより、公開鍵暗号方式よりも高速に暗号化処理を行なうことができるものである。また、大量の暗号文と平文の組を利用する差分攻撃法や線形攻撃法に対して、１回の通信に使用される暗号文と平文の組は、１組か数組のごく少ないものであるので、差分攻撃法や線形攻撃法に必要な数の暗号文と平文の組を入手するには非常に時間がかかるために安全性に優れたものである。

【００５５】また、請求項６に記載の暗号通信方式によれば、通信データの本文のディジタル署名を送信することによって、通信データと送信者とが正当であることを確認することができるものである。

【図面の簡単な説明】

【図１】本発明に係る暗号通信方式を適用した通信装置の構成を示すブロック図である。

11　　12

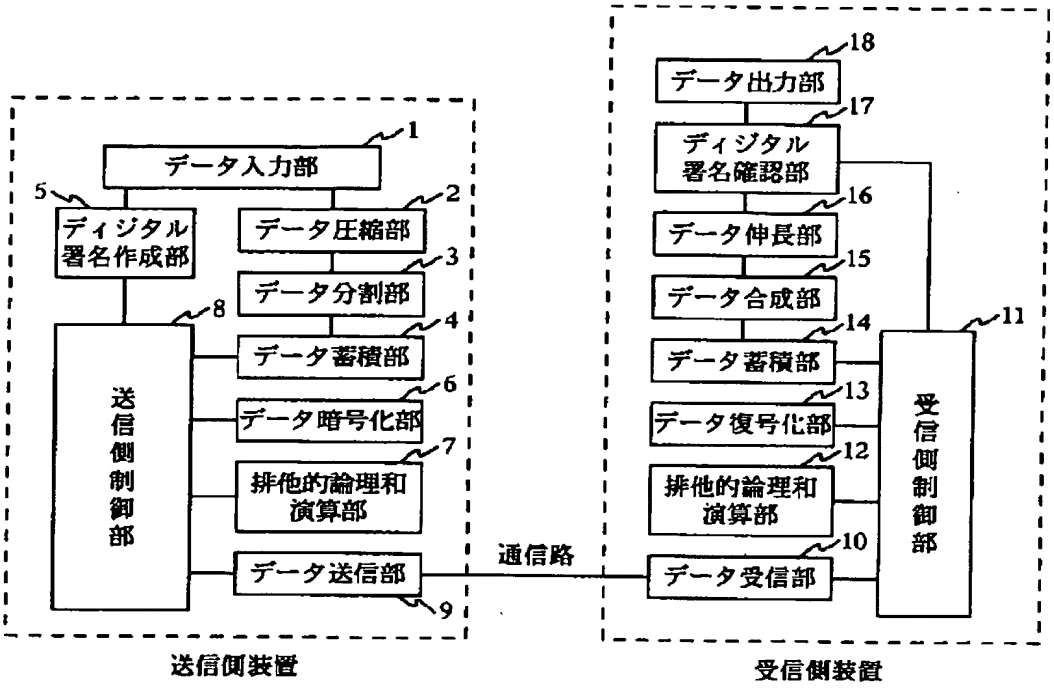
【図２】暗号通信方式の送信手順を示すフローチャートである。

【図３】暗号通信方式の受信手順を示すフローチャートである。

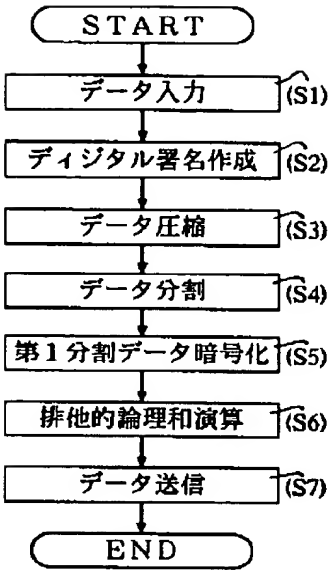
【符号の説明】

２　データ圧縮部
３　データ分割部
５　ディジタル署名生成部
６　データ暗号化部
７　排他的論理和演算部
８　送信側制御部
９　データ送信部
１０　データ受信部
１１　受信側制御部
１２　排他的論理和演算部
１３　データ復号化部
１５　データ合成部
１６　データ伸長部
１７　ディジタル署名確認部

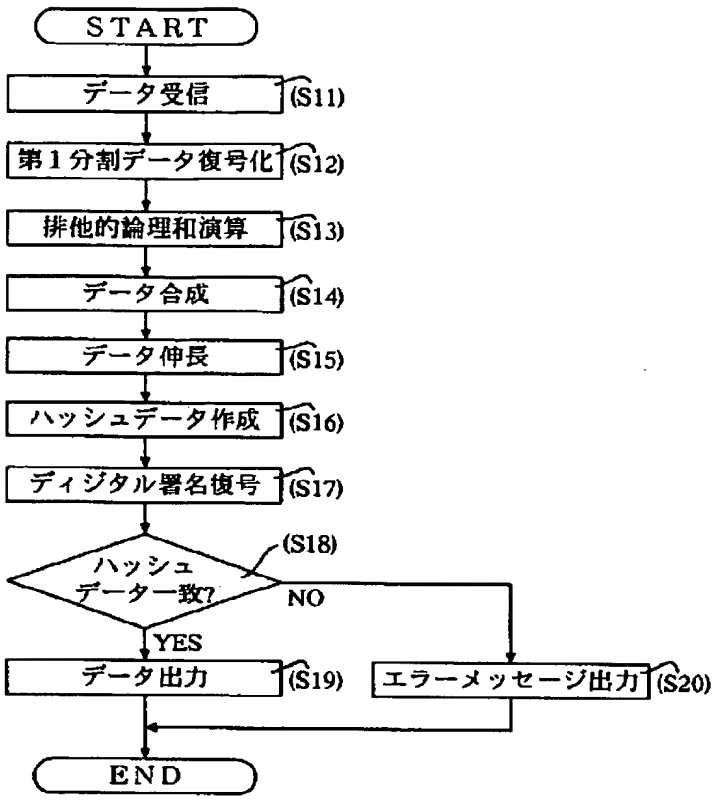
【図１】



【図２】


START
データ入力
(S1)
ディジタル署名作成
(S2)
データ圧縮
(S3)
データ分割
(S4)
第１分割データ暗号化
(S5)
排他的論理和演算
(S6)
データ送信
(S7)
END

【図３】


START
データ受信
(S11)
第１分割データ復号化
(S12)
排他的論理和演算
(S13)
データ合成
(S14)
データ伸長
(S15)
ハッシュデータ作成
(S16)
ディジタル署名復号
(S17)
ハッシュ
データ一致?
(S18)
NO
YES
データ出力
(S19)
エラーメッセージ出力
(S20)
END